

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-276345

(43)Date of publication of application : 06.12.1991

(51)Int.Cl.

G06F 12/14  
G06F 15/78

(21)Application number : 02-077446

(71)Applicant : TOSHIBA CORP  
TOSHIBA MICRO ELECTRON KK

(22)Date of filing : 27.03.1990

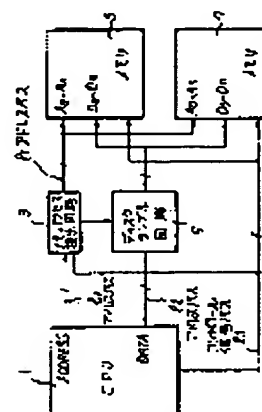
(72)Inventor : SAITO YASUO

## (54) MICROCONTROLLER

## (57)Abstract:

PURPOSE: To prevent the decoding and the alteration of programs and data by decoding the ciphered program data stored in a memory via a descrambling means and actuating a CPU based on the decoded program data.

CONSTITUTION: A CPU 1 performs the control via an address bus signal I1 and a control signal I3 so as to send the cipher decoding key data stored in a memory 7 to a descrambling circuit 9. Then a memory access detection circuit 3 detects an access applied to a memory 5 from the CPU 1 and sends a detection signal to the circuit 9. Thus the circuit 9 is set in an enable state and inverts the data Di kept on a data line. The descrambled data are sent to the CPU 1 and executed there. Thus it is possible to attain a system having high security.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the  
examiner's decision of rejection or application converted  
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of  
rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

**THIS PAGE BLANK (USPTO)**

## ⑫ 公開特許公報(A)

平3-276345

⑤ Int. Cl.<sup>5</sup>G 06 F 12/14  
15/78

識別記号

3 2 0 B  
5 1 0 F

庁内整理番号

7165-5B  
7530-5L

⑬ 公開 平成3年(1991)12月6日

審査請求 有 請求項の数 1 (全4頁)

⑭ 発明の名称 マイクロコントローラ

⑯ 特 願 平2-77446

⑰ 出 願 平2(1990)3月27日

⑱ 発 明 者 斎 藤 靖 夫 神奈川県川崎市川崎区駅前本町25番地1 東芝マイクロエレクトロニクス株式会社内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 出 願 人 東芝マイクロエレクトロニクス株式会社 神奈川県川崎市川崎区駅前本町25番地1

㉑ 代 理 人 弁理士 佐藤 一雄 外3名

## 明 細 書

## 1. 発明の名称

マイクロコントローラ

## 2. 特許請求の範囲

プログラムデータが反転の暗号をかけられた状態で格納される第1のメモリと、この第1のメモリに格納されるプログラムデータにかけらる暗号を解読するのに必要なキーデータが格納される第2のメモリと、前記第1及び第2のメモリにデータを書き込んだり、読み込んだりすることを制御するCPUと、このCPUが前記第1のメモリにアクセスしているときに前記第2のメモリに格納されているキーデータに基づいて前記第1のメモリに格納されているプログラムデータにかけられている暗号を解くディスクリンブル手段とを備え、前記CPUはこのディスクリンブル手段によって暗号解読されたプログラムデータに基づいて動作することを特徴とするマイクロコントローラ。

## 3. 発明の詳細な説明

## 〔発明の目的〕

## (産業上の利用分野)

本発明はマイクロコントローラに関するものであって、特にセキュリティを必要とするICカードやデータバンク等に使用されるものである。

## (従来の技術)

従来のマイクロコントローラにおいては、プログラムのセキュリティが考慮されておらず、メモリに記憶されたプログラムによって直接マイクロコントローラが動作していた。

## (発明が解決しようとする課題)

このようなマイクロコントローラにおいては、メモリに記憶されたプログラムの解読や改ざんが容易にできるため、ハイセキュリティが要求されるICカードや、データバンクに使用するにはあまり具合のいいものではなかった。

本発明は上記事情を考慮してなされたものであって、プログラムやデータの解読や改ざんを可及的に阻止することのできるマイクロコントローラ

を提供することを目的とする。

〔発明の構成〕

(課題を解決するための手段)

本発明のマイクロコントローラは、プログラムデータの一部分が反転の暗号をかけられた状態で格納される第1のメモリと、この第1のメモリに格納されるプログラムデータにかけらる暗号を解読するのに必要なキーデータが格納される第2のメモリと、第1及び第2のメモリにデータを書き込んだり、読み込んだりすることを制御するCPUと、このCPUが第1のメモリにアクセスしているときに第2のメモリに格納されているキーデータに基づいて第1のメモリに格納されているプログラムデータにかけられている暗号を解くディスクランブル手段とを備え、CPUはこのディスクランブル手段によって暗号解読されたプログラムデータに基づいて動作することを特徴とする。

(作 用)

このように構成された本発明のマイクロコントローラによれば、第2のメモリに格納されている

キーデータに基づいて第1のメモリに格納されている暗号のかけられたプログラムデータがディスクランブル手段によって解読され、この解読されたプログラムデータに基づいてCPUが動作する。これにより本発明のマイクロコントローラはプログラム等の解読や改ざんを可及的に阻止することができ、セキュリティの高いシステムを構築することができる。

(実施例)

第1図に本発明によるマイクロコントローラの一実施例の構成を示す。この実施例のマイクロコントローラはCPU1と、メモリアクセス検出回路3と、メモリ5、7と、ディスクランブル回路9とを備えている。メモリ5にはメインプログラムがスクランブル、すなわちデータの一部分が反転の暗号をかけられた状態で格納されている。メモリ7はメモリ5のデータにかけられている暗号を解読するのに必要なキーとなるデータが格納されている。メモリアクセス検出回路3はCPU1からアドレスバス1を介して送られてくるアドレ

ス信号及び3を介して送られてくるコントロール信号に基づいてCPU1がメモリ5をアクセス中であることを検出する。ディスクランブル回路9はメモリ7に格納されているキーデータに基づいてCPU1によってアクセスされているメモリ5のデータをディスクランブル、すなわち暗号を解く処理を行う。このディスクランブル回路9の一具体例を第2図に示す。この具体例のディスクランブル回路9はキーデコード21と、メモリ5に格納されたnビットのプログラムコード又はデータコードD<sub>0</sub>～D<sub>n</sub>の各ビットデータD<sub>i</sub> (i=1, …, n) のデータラインに対して設けられる暗号解読回路S<sub>i</sub> (i=1, …, n) とを有している。又、暗号解読回路S<sub>i</sub>はフリップフロップ(F/Fともいう)Fと、2個のAND回路及び2個のNOR回路からなるデータ反転回路INVとからなっている。

次に、本実施例の作用を第1図及至第3図を参照して説明する。まずメモリ7に格納されている暗号解読のキーデータがディスクランブル回路9

に送られるようにアドレス信号バス1及びコントロール信号バス3を介してCPU1が制御する。すると、上記キーデータはディスクランブル回路9のキーデコード21に送られてデコードされ、このデコードされた信号に基づいて暗号解読回路S<sub>i</sub> (i=1, …, n) のフリップフロップFが“1”又は“0”にセットされる(第3図ステップF31、F32参照)。次にメモリ5をCPU1がアクセスすると、これをメモリアクセス検出回路3が検出し、検出信号をディスクランブル回路9に送る(第3図ステップF33参照)。するとディスクランブル回路9がイネーブル状態になる(第3図ステップF34参照)。この時、フリップフロップFが“1”にセットされた暗号解読回路S<sub>i</sub>においては、データ反転回路INVのイネーブル信号が“1”となってこの暗号解読回路S<sub>i</sub>に接続されたデータライン上のデータD<sub>i</sub>の反転処理が行われ、フリップフロップFが“0”にセットされた暗号解読回路S<sub>j</sub>においては、この暗号解読回路S<sub>j</sub>に接続されたデータラ

イン上のデータ $D_j$ の反転処理が行われない(第3図ステップF35参照)。このようにディスクランブルされたデータ $D_1 \sim D_n$ はCPU1に送られて実行される。なお、CPU1がメモリ7をアクセスするときはディスクランブル回路全体がディスエイブル(disable)になり、データはディスクランブルされずにメモリ7上のデータはそのままCPU1に送られる。

以上述べたように本実施例によれば、メモリ5に格納されてスクランブルされたプログラム又はデータは、メモリ7に格納されているキーデータを用いてディスクランブル回路9によって暗号解読され、この暗号解読されたプログラム又はデータによってCPU1が動作する。これにより本実施例のマイクロコントローラはプログラム又はデータの解読や改ざんを可及的に阻止できるものとなる。

更に、何種類かの暗号解読のキーデータをメモリ7に格納しておけば、ひとつのプログラムに何種類もの暗号をかけることができるので第三者によ

る暗号解読を一層困難なものとすることができる。

又、ハードウェアで設計されているディスクランブル回路をソフトウェアで自由に操作できるので、ソフトウェアにかけられる暗号の種類に合せてハードを変更する必要がない。更に暗号解読のキーデータはハードウェアを変更することなく、ソフトウェアで決定することが可能となり、これによりソフトウェア設計者が暗号解読のキーデータをハードウェア設計者に知らせることなしに決定することができ、セキュリティが高く、しかも汎用性のあるシステムを実現することができる。

#### 【発明の効果】

本発明によれば、プログラムやデータの解読や改ざんを可及的に防止することができ、セキュリティの高いシステムを構築することができる。

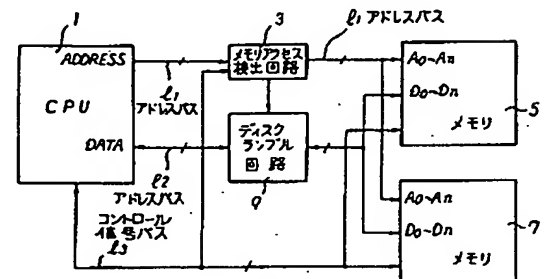
#### 4. 図面の簡単な説明

第1図は本発明のマイクロコントローラの一実施例の構成を示すブロック図、第2図は本発明にかかるディスクランブル回路の一具体例を示す回

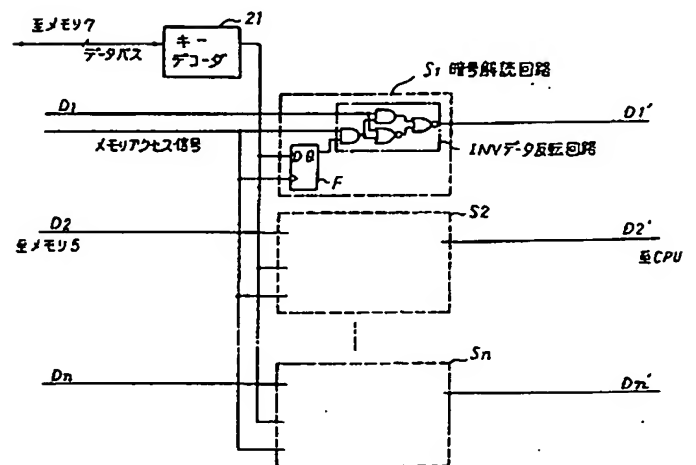
路図、第3図は実施例の作用を説明するフローチャートである。

1…CPU、3…メモリアクセス検出回路、5、7…メモリ、9…ディスクランブル回路。

出願人代理人 佐藤 一 雄



第1図



第2図

平成 3 年 1 月 16 日

特許庁長官 植松 敏 殿

1 事件の表示

平成 2 年特許願第 77446 号

2 発明の名称

マイクロコントローラ

3 補正をする者

事件との関係 特許出願人

(307) 株式会社 東芝 (ほか 1 名)

4 代理人 (郵便番号 100)

東京都千代田区丸の内三丁目2番3号  
[電話東京 (3211)2321 大代表]

6428 弁理士 佐 藤

5 補正命令の日付

発送日 平成 年 月 日

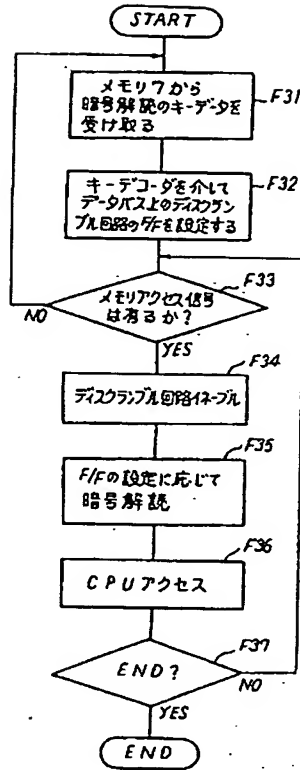
6 補正により する請求項の数

7 補正の対象

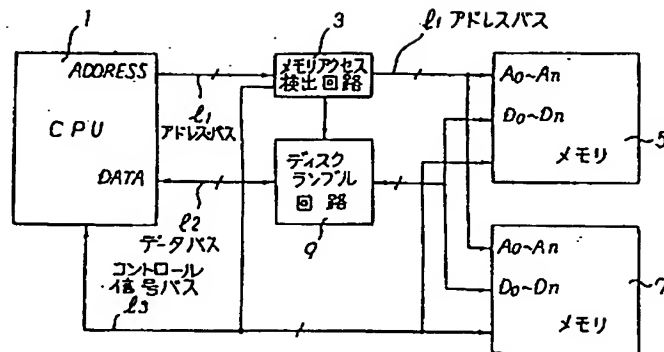
図 面

8 補正の内容

図面中、第1図を別紙の通り訂正する。



第3図



第1図